[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/14
H04L 9/08 G09C 1/00
G11B 20/10

[12]发明专利申请公开说明书

[21]申请号 00134573.7

[43]公开日 2001年8月8日

[11]公开号 CN 1307284A

[22]申请日 2000.12.11 [21]申请号 00134573.7

[30]优先权

[32]2000.1.21 [33]JP [31]012733/2000

[32]2000.2.28 [33]JP [31]051204/2000

[71]申请人 日本胜利株式会社

地址 日本神奈川县

[72]发明人 黑岩俊夫 菅原隆幸 猪羽涉
上田健二朗 日幕诚司

[74]专利代理机构 中原信达知识产权代理有限责任公司

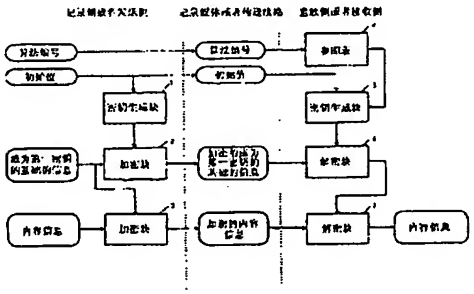
代理人 谢丽娜 余 朦

权利要求书8页 说明书10页 附图页数2页

[54]发明名称 内容信息的传送与记录方法、装置和媒体及解密方法与装置

[57]摘要

根据本发明，仅用提供给加密方的知识，在解密方不能根据所指 定的各个算法编号来分别确定用于加密的密钥生成算法。本发明传送 或者记录下列信息：使用从成为第一密钥基础的信息所生成的第一密 钥对内容信息进行加密得到的加密内容信息、使用第二密钥对上述成 为第一密钥基础的信息加密得到的加密的成为第一密钥基础的信息、用于确定上述预定的密钥生成算法的算法确定信息、表示上述初始值 的初始值信息。



ISSN1008-4274

00.12.11

权 利 要 求 书

1. 一种内容信息传送方法，其特征在于，传送下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

2. 一种内容信息记录方法，其特征在于，记录下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

3. 一种内容信息传送装置，其特征在于，包括：

内容信息加密装置，使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密，并输出加密内容信息；

第一密钥信息加密装置，使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密，并输出加密的成为第一密钥基础的信息；以及

传送装置，传送上述加密内容信息、上述加密的成为第一密钥基础的信息、上述用于确定预定的密钥生成算法的算法确定信息以及表示上述初始值的初始值信息。

00.12.11

4. 一种内容信息记录装置，其特征在于，包括：

内容信息加密装置，使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密，并输出加密内容信息；

第一密钥信息加密装置，使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密，并输出加密的成为第一密钥基础的信息；以及

记录装置，把上述加密内容信息、上述加密的成为第一密钥基础的信息、上述用于确定预定的密钥生成算法的算法确定信息以及表示上述初始值的初始值信息记录到媒体上。

5. 一种传送媒体，其特征在于，传送下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

6. 一种记录媒体，其特征在于，记录下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

7. 根据权利要求 3 记载的内容信息传送装置或者权利要求 4 记载的内容信息记录装置，其特征在于，上述第一密钥信息加密装置包

括基于所提供的初始值并按照预定的密钥生成算法来生成第二密钥的密钥生成装置，该密钥生成装置具有使用特定的不可约原始多项式的线性反馈移位寄存器。

8. 一种内容信息传送方法，其特征在于，传送下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

9. 一种内容信息记录方法，其特征在于，记录下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

10. 一种内容信息传送装置，其特征在于，包括：

内容信息加密装置，使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密，并输出加密内容信息；

第一密钥信息加密装置，使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密，并输出加密的成为第一密钥基础的信息；

传送装置，传送上述加密内容信息、上述加密的成为第一密钥基础的信息、上述用于确定预定的密钥生成算法的算法确定信息以及表

示上述初始值的初始值信息。

11. 一种内容信息记录装置，其特征在于，包括：

内容信息加密装置，使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密，并输出加密内容信息；

第一密钥信息加密装置，使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密，并输出加密的成为第一密钥基础的信息；以及

记录装置，把上述加密内容信息、上述加密的成为第一密钥基础的信息、上述用于确定预定的密钥生成算法的算法确定信息以及表示上述初始值的初始值信息记录到媒体上。

12. 一种传送媒体，其特征在于，传送下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密得到的加密的成为第一密钥基础的信息；以及

用于确定上述预定的密钥生成算法的算法确定信息；

表示上述初始值的初始值信息。

13. 一种记录媒体，其特征在于，记录下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

14. 根据权利要求 10 记载的内容信息传送装置或者权利要求 11 记载的内容信息记录装置，其特征在于，上述第一密钥信息加密装置包括基于所提供的初始值并按照预定的密钥生成算法来生成第二密钥的密钥生成装置，该密钥生成装置具有使用特定的不可约原始多项式的线性反馈移位寄存器。

15. 一种内容信息解密方法，使用以下信息来对内容信息进行解密：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密而得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；和

表示上述初始值的初始值信息，

其特征在于，

根据上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法，

从上述初始值信息来得到上述初始值，使用该初始值，按照上述所确定的预定的密钥生成算法来生成上述第二密钥，

根据该生成的第二密钥，来对上述加密的成为第一密钥基础的信息进行解密，而得到上述成为第一密钥基础的信息，以及

从该成为第一密钥基础的信息来生成上述第一密钥，根据该第一密钥对上述加密内容信息进行解密，来得到上述内容信息。

16. 一种内容信息解密装置，使用以下信息来对内容信息进行解密：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第

二密钥，来对上述成为第一密钥基础的信息进行加密的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；和

表示上述初始值的初始值信息，

其特征在于，设有：

第二密钥生成装置，按照上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法，同时，从上述初始值信息来得到上述初始值，使用该初始值，按照上述所确定的预定的密钥生成算法来生成上述第二密钥；

第一密钥信息解密装置，根据该生成的第二密钥，来对上述加密的成为第一密钥基础的信息进行解密，而得到上述成为第一密钥基础的信息；以及

内容信息解密装置，从该解密的成为第一密钥基础的信息来生成上述第一密钥，根据该第一密钥对上述加密内容信息进行解密，来得到上述内容信息。

17. 根据权利要求 16 记载的内容信息解密装置，其特征在于，

上述第二密钥生成装置包括多个密钥生成算法，从该多个密钥生成算法中根据上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法。

18. 根据权利要求 17 记载的内容信息解密装置，其特征在于，

上述第二密钥生成装置中的上述多个密钥生成算法是分别基于不同的原始多项式的，上述第二密钥生成装置包括线性反馈移位寄存器，根据按照上述算法确定信息所确定的预定的密钥生成算法中的原始多项式，能够设定成为反馈的对象的寄存器位置。

19. 一种内容信息解密方法，使用以下信息来对内容信息进行解密：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进

行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；和

表示上述初始值的初始值信息，

其特征在于，

根据上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法，

从上述初始值信息来得到上述初始值，使用该初始值，按照上述所确定的预定的密钥生成算法来生成上述第二密钥，

根据该生成的第二密钥，来对上述加密的成为第一密钥基础的信息进行解密，而得到上述成为第一密钥基础的信息，以及

从该成为第一密钥基础的信息来生成上述第一密钥，根据该第一密钥对上述加密内容信息进行解密，来得到上述内容信息。

20. 一种内容信息解密装置，使用以下信息来对内容信息进行解密：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行部分加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；和

表示上述初始值的初始值信息，

其特征在于，设有：

第二密钥生成装置，根据上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法，同时，从上述初始值信息来得到上述初始值，使用该初始值，按照上述所确定的预定的密钥生成算法来生成上述第二密钥；

第一密钥信息解密装置，根据该生成的第二密钥，来对上述加密的成为第一密钥基础的信息进行解密，而得到上述成为第一密钥基础的信息；以及

内容信息解密装置，从该解密的成为第一密钥基础的信息来生成上述第一密钥，根据该第一密钥对上述加密内容信息进行解密，来得到上述内容信息。

21. 根据权利要求 20 记载的内容信息解密装置，其特征在于，

上述第二密钥生成装置包括多个密钥生成算法，从该多个密钥生成算法中根据上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法。

22. 根据权利要求 21 记载的内容信息解密装置，其特征在于，

上述第二密钥生成装置中的上述多个密钥生成算法是分别基于不同的原始多项式的，上述第二密钥生成装置包括线性反馈移位寄存器，根据按照上述算法确定信息所确定的预定的密钥生成算法中的原始多项式，能够设定成为反馈的对象的寄存器位置。

00.12.11

说　明　书

内容信息的传送与记录方法、装置和媒体及解密方法与装置

本发明涉及用于传送、记录内容密钥和使用该内容密钥所加密的加密内容信息的内容信息传送方法、内容信息记录方法、内容信息传送装置、内容信息记录装置、传送媒体、记录媒体、内容信息解密方法以及内容信息解密装置。而且，本发明的目的是提供即使在仅使用有利于处理速度的对称加密的情况下也能够更有力地防止内容信息的非法重放（解密）、复制来强化著作权保护的内容信息传送方法、内容信息记录方法、内容信息传送装置、内容信息记录装置、传送媒体、记录媒体、内容信息解密方法以及内容信息解密装置。

随着加密技术的发展，作为利用网络来分送音频和视频的数字数据的有用的方法，有日本专利公开公报特开平 10-269289 的数字内容发布管理方法、数字内容重放方法及装置。在该发明中，在数字内容的配发方，对数字内容经加密以及压缩进行加工，把该加工的数字内容和加密的内容密钥以及加密的缴费信息发送给通信对方。接着，给权利所有者分配根据从通信对方所发送的内容使用信息而征收的使用费。另一方面，在数字内容的重放侧，用内容密钥对该加工的数字内容进行解密，同时进行解压缩和重放。同时，根据内容的使用而向配发方发送缴费信息的扣除额度和内容使用信息，这样，能够挪动所记录的内容。

而且，在日本专利公开公报特开平 10-283268 的信息记录媒体、记录装置、信息传送系统、密码解读装置中，记录加密的加密信息、对用于把该加密信息解密为原始信息的密钥信息进行加密的加密密钥信息，其中，在上述加密密钥信息中附加记录在非加密的状态下对上述加密信息进行解密时的条件信息。即，由于在加密密钥信息的控制

信息内，包含机器信息和区域信息，因此，能做到防止在用户方把加密的信息直接复制到 HDD 和光盘中进行非法使用。

加密方式大致分为：使用共同密钥的对称加密方式和使用公开密钥、秘密密钥的非对称加密方式。如特开平 10-283268 所示的那样，当传送音频和视频等大容量的数字数据（内容信息）时，给内容信息设定共同密钥（内容密钥），进行有利于处理速度的对象加密，同时，给使用的内容密钥另外进行非对称加密来进行传送。但是，非对称加密主要在处理速度的快慢上存在缺点。因此，也可以使用这样的方法：在加密装置和解密装置中设定共同的上位密钥所谓主密钥，使用主密钥对内容密钥进行对称加密来进行传送。

但是，在上述的仅使用对称加密的现有方式中，在制造加密装置侧和制造解密装置侧，与加密方式相关的知识是一致的。即，在制造任一个装置时，是以知道主密钥、内容和内容密钥的加密算法为前提条件的。

这就意味着不是不能用构成加密装置的知识来构成解密装置，而是担心会存在与防止非法复制来保护著作权的加密目的不相称的非法解密装置的流通。

本发明的目的是提供内容信息传送方法、记录方法、传送装置、记录装置、传送媒体、记录媒体、解密方法以及解密装置，即使在仅使用有利于处理速度的对称加密的情况下，仅用提供给加密方的知识，在解密方，也不能根据所指定的各个算法的编号来分别确定用于加密的密钥生成算法，从而能够更有力地防止内容信息的非法重放（解密）、复制，由此强化著作权保护。

因此，为了解决上述问题，本发明提供下列方法・装置：

（1）一种内容信息传送方法，其特征在于，传送下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

（2）一种内容信息记录方法，其特征在于，记录下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

（3）一种内容信息传送装置，其特征在于，包括：

内容信息加密装置，使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密，并输出加密内容信息；

第一密钥信息加密装置，使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密，并输出加密的成为第一密钥基础的信息；以及

传送装置，传送上述加密内容信息、上述加密的成为第一密钥基础的信息、上述用于确定预定的密钥生成算法的算法确定信息以及表示上述初始值的初始值信息。

（4）一种内容信息记录装置，其特征在于，包括：

内容信息加密装置，使用从成为第一密钥基础的信息所生成的第一密钥，来对内容信息进行加密，并输出加密内容信息；

第一密钥信息加密装置，使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密，并输出加密的成为第一密钥基础的信息；以及

记录装置，把上述加密内容信息、上述加密的成为第一密钥基础的信息、上述用于确定预定的密钥生成算法的算法确定信息以及表示上述初始值的初始值信息记录到媒体上。

（5）一种传送媒体，其特征在于，传送下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

（6）一种记录媒体，其特征在于，记录下列信息：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；以及

表示上述初始值的初始值信息。

（7）根据上述（3）记载的内容信息传送装置或者上述（4）记载的内容信息记录装置，其特征在于，上述第一密钥信息加密装置包括基于所提供的初始值并按照预定的密钥生成算法来生成第二密钥的密钥生成装置，该密钥生成装置具有使用特定的不可约原始多项式的线性反馈移位寄存器。

（8）一种内容信息解密方法，使用以下信息来对内容信息解密：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密而得到的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；和

表示上述初始值的初始值信息，

其特征在于，

根据上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法，

从上述初始值信息来得到上述初始值，使用该初始值，按照上述所确定的预定的密钥生成算法来生成上述第二密钥，

根据该生成的第二密钥，来对上述加密的成为第一密钥基础的信息进行解密，而得到上述成为第一密钥基础的信息，以及

从该成为第一密钥基础的信息来生成上述第一密钥，根据该第一密钥对上述加密内容信息进行解密，来得到上述内容信息。

（9）一种内容信息解密装置，使用以下信息来对内容信息解密：

使用从成为第一密钥基础的信息所生成的第一密钥对内容信息进行加密得到的加密内容信息；

使用基于所提供的初始值并按照预定的密钥生成算法所生成的第二密钥，来对上述成为第一密钥基础的信息进行加密的加密的成为第一密钥基础的信息；

用于确定上述预定的密钥生成算法的算法确定信息；和

表示上述初始值的初始值信息，

其特征在于，设有：

第二密钥生成装置，按照上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法，同时，从上述初始值信息来得

到上述初始值，使用该初始值，按照上述所确定的预定的密钥生成算法来生成上述第二密钥；

第一密钥信息解密装置，根据该生成的第二密钥，来对上述加密的成为第一密钥基础的信息进行解密，而得到上述成为第一密钥基础的信息；以及

内容信息解密装置，从该解密的成为第一密钥基础的信息来生成上述第一密钥，根据该第一密钥对上述加密内容信息进行解密，来得到上述内容信息。

（10）在上述（9）记载的内容信息解密装置，其特征在于，

上述第二密钥生成装置包括多个密钥生成算法，从该多个密钥生成算法中根据上述算法确定信息来确定用于生成上述第二密钥的上述预定的密钥生成算法。

（11）在上述（10）记载的内容信息解密装置，其特征在于，

上述第二密钥生成装置中的上述多个密钥生成算法是分别基于不同的原始多项式的，上述第二密钥生成装置包括线性反馈移位寄存器，根据按照上述算法确定信息所确定的预定的密钥生成算法中的原始多项式，能够设定成为反馈的对象的寄存器位置。

本发明的这些和其他的目的、优点及特征将通过结合附图对本发明的实施例的描述而得到进一步说明。在这些附图中：

图 1 是表示本发明的一个实施例的简要构成的图；

图 2 是表示记录侧或者发送侧的密钥生成块的一个例子的图。

在图 1 中表示了本发明的内容信息记录装置或者内容信息传送装置、内容信息解密装置的一个实施例的简要构成。而且，在本说明中，把磁记录媒体、光记录媒体、半导体存储器等称为记录媒体，把光缆、电线、无线传送线路等传送信号的传送媒体称为传送线路。

首先，对记录侧或者发送侧进行说明。在记录侧或者发送侧中，包括：用于生成第二密钥的密钥生成块 1、根据上述第二密钥对成为第一密钥（内容密钥）的基础的信息进行加密的加密块 2 以及从成为第一密钥（内容密钥）的基础的信息来生成第一密钥（内容密钥）并对内容信息加密的加密块 3。

向记录侧或者发送侧的装置的输入是：

· 在重放侧或者接收侧，用于指定为了生成第二密钥的密钥生成算法，与在密钥生成块 1 内所使用的密钥生成算法相对应的算法编号；

· 提供给密钥生成块 1 的初始值；

· 用于生成在内容信息的加密中所使用的第一密钥（内容密钥）的成为第一密钥基础的信息；以及

· 内容信息。

作为密钥生成块 1 的输出的第二密钥起到用于对成为第一密钥（内容密钥）的基础的信息进行加密的上位密钥的作用，其随机地并且通过初始值而发生较大的变化来求出。

在图 2 中表示了密钥生成块 1 的一个实施例。在该实施例中，由以下部分构成：具有预定位数 N（在图中，N=8）的移位寄存器（r1～r8）和用于得到来自预定的寄存器位置的“异或”的门群（g1～g8）、系数设定总线和初始值设定总线。把“异或”的结果设定到最低位寄存器的这样的电路被称为线性反馈移位寄存器（LFSR）。初始值输入通过初始值总线被设定在各个寄存器中，同时，通过系数输入来设定各个门的开关状态。然后，对移位寄存器提供时钟，而得到来自最上位寄存器的输出。

为了最有效地得到随机的输出，设定系数必须与 N 次的原始多项式相对应。例如，在 N=8 中，是 8 次的原始多项式之一，

$x^8+x^7+x^2+x+1$ 【式 1】

当使用式 1 时，对应于（g8、g7、g6、g5、g4、g3、g2、g1），向各个门输入系数（1，1，0，0，0，0，1，1）。接着，初始值设定被选择为 0 以外的值。来自最上位寄存器的输出成为被称为 M 系列的具有高随机性的比特串，但是，由于与 LFSR 性质上将来的输出相关的预测是容易的，因此，在输出中包括由具有乘法运算等非线性的函数所产生的变换是理想的。把该输出比特串按预定的格式用于对成为第一密钥（内容密钥）的基础的信息的加密。

对于成为第一密钥基础的信息的加密块 2 和内容信息的加密块 3，可以使用 DES 等公知的加密算法。而且，作为被加密的成为第一密钥基础的信息，可以用第二密钥来对成为第一密钥基础的信息进行全部加密，也可以进行部分加密。（例如，被加密的成为第一密钥基础的信息可以是这样的状态：仅对成为第一密钥基础的信息内的特别重要的部分进行加密，其他部分不进行加密）。

用预定的格式向记录媒体或者传送线路记录或者传送在指定用于生成第二密钥的密钥生成算法中所使用的算法编号、初始值、加密的成为第一密钥基础的信息、加密的内容信息。算法编号相对于上述特定的原始多项式必须是单值的。

而且，初始值和算法编号可以按照预定的函数进行变换来被记录或者传送。（在重放侧或者接收侧，使用预定函数的反函数来得到初始值和算法编号）。

下面对重放侧或者接收侧进行说明。解密装置包括：用于确定用于生成第二密钥的密钥生成算法的参照表 4、用于生成第二密钥的密钥生成块 5、成为第一密钥（内容密钥）的基础的信息的解密块 6 以及从解密的成为第一密钥基础的信息来生成第一密钥（内容密钥）而

对内容信息进行解密的解密块 7。密钥生成块 5 具有与记录侧或者发送侧装置中的相同的构成。对于成为第一密钥（内容密钥）的基础的信息的解密块 6 以及内容信息的解密块 7，与记录侧或者发送侧装置的加密块 2 和 3 分别成对地构成。

为了从算法编号来确定用于生成第二密钥的原始多项式，而设置参照表 4。参照表 4 具体地由 ROM 所实现，可以把算法编号作为输入地址，把与原始多项式相对应的系数列作为输出。在表 1 中表示了原始多项式为 8 次时的参照表的构成例子。下面说明解密装置的动作。

【表 1】

表 1 参照表的一例

算法编号	系数列	原始多项式
0	(1,1,0,0,0,0,1,1)	$x^8+x^7+x^2+x+1$
1	(1,0,0,0,1,1,1,0)	$x^8+x^4+x^3+x^2+1$
2	(1,0,1,1,0,1,0,0)	$x^8+x^6+x^5+x^3+1$
3	(1,1,1,1,0,0,1,1)	$x^8+x^7+x^6+x^5+x^2+x+1$
4	(1,0,0,1,0,1,0,1)	$x^8+x^5+x^3+x+1$
5	(1,0,1,1,0,0,1,0)	$x^8+x^6+x^5+x^2+1$
6	(1,0,1,1,0,0,0,1)	$x^8+x^6+x^5+x+1$
7	(1,0,1,0,1,1,1,1)	$x^8+x^6+x^4+x^3+x^2+x+1$

解密装置向参照表 4 输入来自记录媒体或者传送线路的算法编号，而得到对应的系数列。把该系数列和来自记录媒体或者传送线路的初始值输入到密钥生成块 5 中，与记录侧或者发送侧相同，在进行了对寄存器的初始值设定和门状态的设定之后，提供闩锁，而得到输出的比特串。按预定的格式使用输出比特串来作为成为第一密钥（内容密钥）的基础的信息的解密密钥，在解密块 6 中，把来自记录媒体或者传送线路的信息解密为成为第一密钥（内容密钥）的基础的信息。而且，从该解密的成为第一密钥基础的信息来生成第一密钥（内容密

钥），在解密块 7 中对来自记录媒体或者传送线路的加密内容信息进行解密。

在实施过程中，从保持加密强度的观点出发，希望把解密装置整体做成难以被解析的水平。特别是，参照表 4 需要注意的是：使内容读出到解密装置之外的可能性变低。作为最佳实施例，把解密装置整体做成一体的 LSI。

这样，在本实施例中，由于参照表 4 仅提供给解密侧，就不可能制作出具有以下功能的解密装置：用仅提供给加密侧的知识按照所指定的算法编号，来变更密钥生成算法。这样，具有防止制作非法解密装置的效果。而且，当发现了仅实现在加密阶段所使用的密钥生成算法的非法解密装置的情况下，在加密侧变更密钥生成算法的同时，变更传送的算法编号，由此，能够进行用非法解密装置不能进行解密的内容的发送、发布。

而且，在上述实施例的记录或者传送装置以及解密装置中，虽然举出了在成为第一密钥（内容密钥）的基础的信息和密钥生成块使用输出的上位密钥（第二密钥）的同时，将加密块、解密块做成两段的例子，但是，可以准备 M 个成为第一密钥（内容密钥）的基础的信息，而把成为第一密钥（内容密钥）的基础的信息的加密做成 M 段。在此情况下，在媒体或者传送线路中，能够记录、传送 M 个加密的成为第一密钥基础的信息。

如以上那样，根据本发明，即使在仅使用对于处理速度有利的对称加密的情况下，仅用提供给加密方的知识，在解密方，也不能根据所指定的各个算法的编号来分别确定用于加密的密钥生成算法，由此，能够更有力地防止内容信息的非法重放（解密）、复制，来强化著作权保护。

说 明 书 附 图

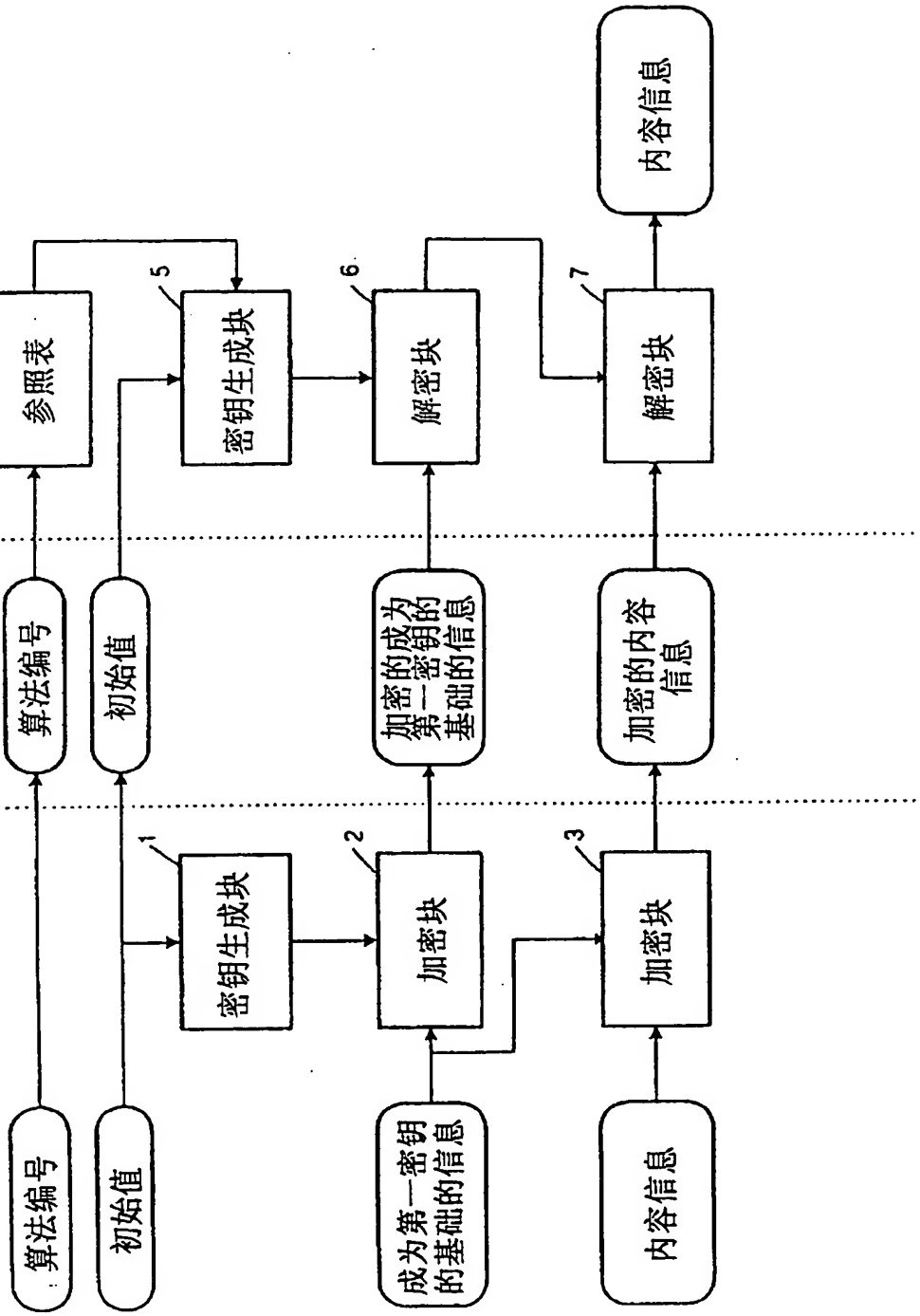

记录侧或者发送侧
记录媒体或者传送线路
重放侧或者接收侧
算法编号
初始值
密钥生成块
1
加密块
2
加密块
3
参照表
4
密钥生成块
5
解密块
6
解密块
7
成为第一密钥的基础的信息
内容信息
算法编号
初始值
加密的成为第一密钥的基础的信息
加密的内容信息
内容信息

图1

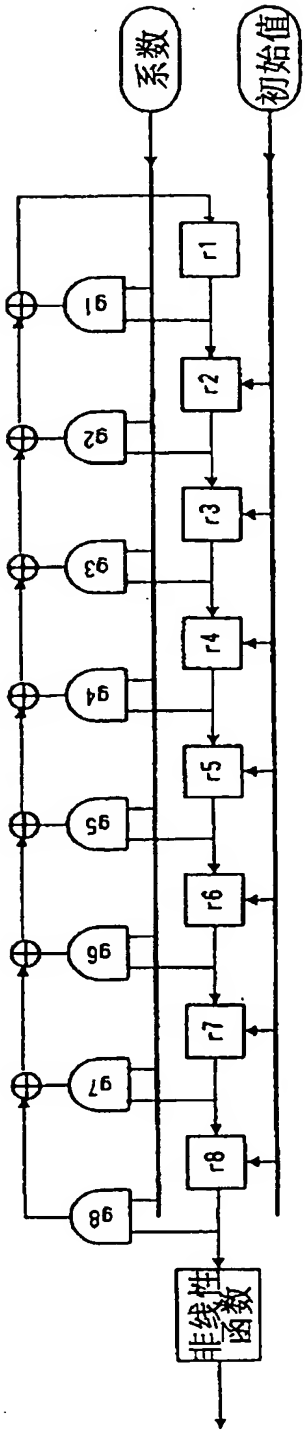


图2 密钥生成块的实施例